Grosvenor Place
Level 15, 225 George Street
Sydney NSW 2000
Australia

T +61 2 9816 3880

www.custos.ltd

17 October 2025

Senator Helen Polley
Chair
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

via email: le.committee@aph.gov.au

Dear Senator Polley

Submission to the re-referred Inquiry into the Capability of Law Enforcement to Respond to Money Laundering and Financial Crime

Thank you for the opportunity to contribute to the Committee's critical inquiry into Australia's law enforcement capability to respond to money laundering and financial crime.

With over two decades of experience in financial crime risk management - spanning governance, anti-money laundering and counter-terrorism financing (AML/CTF), sanctions, fraud, and cybercrime, I have observed the increasing sophistication of criminal networks and the persistent operational challenges facing both law enforcement and reporting entities. My experience span both direct roles within financial institutions and advisory positions in professional services, including extensive regulatory remediation following enforcement actions.

This submission, informed by global best practices, comparative regulatory studies, and lessons from public-private sector cooperation, provides a strategic, evidence-based perspective on:

- The evolving scale, typologies, and socio-economic impacts of money laundering in Australia.
- Emerging risks posed by new technologies and value-transfer mechanisms, including virtual assets and cyber-enabled fraud.
- Critical insights into international AML/CTF regimes, inter-agency collaboration models, and their relevance to the Australian context.
- Actionable opportunities to enhance national capability through strengthened intelligence sharing, optimal resource allocation, and data-driven enforcement strategies.

My aim is to support the Committee's deliberations with practical, forward-looking recommendations designed to strengthen Australia's resilience to financial crime, protect the

integrity of our financial system, and promote a proportionate and effective regulatory and enforcement response.

I commend the Committee's ongoing commitment to this vital area. I appeared as an industry witness before the Australian Parliamentary Joint Committee on Law Enforcement's inquiry into financial-related crime (2015). More recently, I made contributions to the development of the United Nations Convention against Cybercrime (2022). I would welcome the opportunity to elaborate further on my submission.

Should the Committee require additional information, or wish for me to appear as a witness at a hearing, please do not hesitate to contact me at [redacted]

We are happy for this submission to be made public.

Thank you for your consideration.

Yours sincerely

Crispin Yuen, CAMS-Audit, CISSP, CISA

Director

(Attachment 1: Submission)
(Attachment 2: About the Author)

Submission to the Parliamentary Joint Committee on Law Enforcement (PJCLE) Inquiry into the Capability of Law Enforcement to Respond to Money Laundering and Financial Crime (2025)

1. Executive Summary

1.1 Australia's law enforcement capability is at an inflection point. Legislative modernisation (AML/CTF Amendment Bill 2024 and Rules 2025), revitalised agency plans (AUSTRAC, ACIC), state-level reforms, and expanded public-private partnership have created momentum. Yet persistent structural gaps, particularly around tranche two entities (legal, real estate, accountants, dealers in precious stones, metals and products), beneficial ownership usability (especially trusts), cyber-enabled fraud, trade-based money laundering (TBML), capital-markets laundering, and virtual assets, continue to be exploited by agile, borderless criminal networks.

1.2 This submission sets out a practical, measurable, proposed plan to convert reform momentum into operational impact. It emphasises five pillars:

1.2.1 Finish the legislative job (coverage, clarity, consistency);

1.2.2 Industrialise intelligence (data, analytics, AI[1] with safeguards);

1.2.3 Out-cooperate adversaries (domestic and cross-border sharing);

1.2.4 Make asset recovery routine (not exceptional); and

1.2.5 Measure what matters (effectiveness, not just activity).

1.3 Ten priority recommendations

1.3.1 Complete and operationalise tranche two regulation with tailored guidance, and uplift funding.

1.3.2 Stand up a national, privacy-by-design, COSMIC[2]-style financial crime information sharing platform (with privacy enhancing technologies (PETs)) that includes banks, payments, Virtual Asset Service Providers (VASPs), and high-risk designated non-financial businesses and professions (DNFPBs).

1.3.3 Deploy an "effectiveness-first" suspicious matter monitoring blueprint (Wolfsberg-aligned[3]) that integrates entity resolution, network analytics, and explainable AI or machine learning models[4].

[1] Artificial Intelligence.
[2] COSMIC stands for "COllaborative Sharing of Money Laundering /TF Information & Cases", The Monetary Authority of Singapore (MAS) launched COSMIC in April 2024, the first centralised digital platform to facilitate sharing of customer information among financial institutions to combat money laundering, terrorism financing and proliferation financing globally.
RUSI, Future of Financial Intelligence Sharing (FFIS)
[3] Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity, Part I: Moving Beyond Automated Transaction Monitoring
Wolfsberg Statement on Effective Monitoring for Suspicious Activity, Part II: Transitioning to Innovation
[4] Explainable AI: AI systems designed to make their decisions transparent and understandable to humans, showing how a model arrives at its predictions rather than functioning as a "black box".

1.3.4 Make beneficial ownership data usable. Implement structured, interoperable standards (e.g., BODS[5]), verified trust-party data (R.25[6]), and near-real-time change logs accessible on legitimate interest.

1.3.5 Establish a National Asset Recovery Tasking & Coordination Function, deepen links to CARIN-style networks[7], with shared targets, Key Performance Indicators (KPIs), and ring-fenced reinvestment of confiscations.

1.3.6 Create a TBML Fusion Cell (ABF/Customs, AUSTRAC, ATO, Home Affairs, DFAT, industry) and embed enhanced trade data elements into intelligence reporting and customs analytics.

1.3.7 Build a national scams and cyber-enabled fraud (CEF) joint operations cadence (AFP, ACIC, ASD, AUSTRAC, states, major platforms, telcos, banks, VASPs) with “stop-the-loss” standard operating procedures (SOPs) and 24/7 rapid response.

1.3.8 Tighten proliferation financing (PF) and sanctions-evasion controls across maritime/shipping registries, virtual assets, gold/stablecoin channels, and capital markets. Require risk programs proportionate to exposure.

1.3.9 Launch a Capital Markets MLTM[8] program (with ASIC and AUSTRAC) on placement-through-markets typologies, wholesale broker risks, and surveillance, know your customer (KYC) uplifts.

1.3.10 Publish and track outcome KPIs (asset denial; seizure to confiscation conversion; SMR[9]-to-outcome rates; disruption of criminal networks; scam loss reduction; FATF effectiveness ratings), with transparent six-monthly reporting.

2. Context and Threat Picture

2.1 Simple: Criminals move fast, share information, and hide in legal structures and digital channels. Our system must be at least as connected and data-driven as theirs.

2.2 Detailed: National risk assessments confirm high money laundering and terrorism financing (ML/TF) risks via professional enablers, opaque legal arrangements (trusts and corporate vehicles), high-value assets (real estate), cash-based placement, TBML, and accelerating cyber-enabled fraud.

Drug markets are resilient. Wastewater analyses and law enforcement data show recovery and diversification post-pandemic.[10] Scam ecosystems (including “pig-butchering”[11], business email compromise (BEC), crypto drainers[12]) weaponise

[5] The Beneficial Ownership Data Standard (BODS) is an open global standard developed by Open Ownership to improve how beneficial ownership data is collected, structured, and shared. It promotes transparency and interoperability, and is adopted by countries such as Canada and the United Kingdom.
[6] Financial Action Task Force (FATF) Recommendation 25: Transparency and beneficial ownership of legal arrangements
[7] Australia is a member of the Asset Recovery Interagency Network - Asia Pacific (ARIN-AP). ARIN-AP is modelled on Camden Assets Recovery Interagency Network (CARIN)
[8] Capital markets connect buyers and sellers of financial assets such as stocks, bonds, and currencies, driving economic growth by linking investors with entities seeking capital. Money Laundering Through Markets (MLTM) refers to using these markets to disguise criminal proceeds as legitimate funds.
[9] Suspicious Matter Report (SMR)
[10] ACIC, Report 24 of the National Wastewater Drug Monitoring Program.
[11] Pig butchering, also known as romance baiting and Sha Zhu Pan, is a scam in which offenders often devote long periods of time to gain the trust of victims before encouraging them to invest in the share market, cryptocurrency or foreign currency exchanges.
[12] A crypto drainer is a scam-as-a-service kit that supplies affiliates with phishing infrastructure (fake sites and malicious smart contracts) that steal victims’ crypto and split the proceeds between the operator and affiliates.

social engineering, AI, and instant payments. Virtual assets are exploited for speed and cross-chain laundering. PF and sanctions evasion use intermediaries, maritime obfuscation, and virtual assets.

The ABCD of Transnational Organised Crime

Transnational organised crime networks are Agile, Borderless, Controlling, and Destructive (ABCD), requiring multi-agency, international, technology-enabled responses.

3. Current Capability - What's working and what's not

3.1 Strengths

3.1.1 Modernising legal framework: AML/CTF Bill 2024 and Rules 2025 (travel rule, transfers of value, enhanced customer due diligence (ECDD), registration).

3.1.2 Public-private partnerships: AUSTRAC's Fintel Alliance expansion; multi-agency taskforces; growing industry readiness.[13]

3.1.3 Agency strategies: AUSTRAC Corporate Plan 2025–29 (data-driven supervision), ACIC Corporate Plan (intelligence integration, partner engagement).

3.1.4 Counter-terrorism financing: coherent national regime; proportionate focus on small-value, digitally-enabled channels; improving PF national risk assessment (NRA) baseline.

3.1.5 State momentum: stronger focus on unexplained wealth, Electronic Gaming Machines (EGMs) risks, and state-level asset confiscation teams.

3.2 Gaps

3.2.1 Coverage and clarity: Incomplete operationalisation for DNFBPs[14]; uneven sector guidance and capacity; trusts transparency remains complex.[15]

3.2.2 Usability of data: Beneficial ownership registries are not yet sufficiently structured, interoperable, verified, or timely for frontline investigations.[16]

3.2.3 Intelligence "industrialisation": Fragmented data, limited entity resolution[17], and rules-heavy monitoring yield high false positives and low signal-to-noise[18].

[13] AUSTRAC, AUSTRAC expands Fintel Alliance to strengthen fight against financial crime.
[14] These sectors are known internationally as Designated Non-Financial Businesses and Professions (DNFBPs) or tranche two in the Australian context.
[15] Asia/Pacific Group on Money Laundering (APGML), APG Yearly Typologies Report 2024; FATF Guidance on Beneficial Ownership and Transparency of Legal Arrangements; Transparency International, Reforming global standards on beneficial ownership transparency; Supplementary Explanatory Memorandum for the AML/CTF Amendment Bill 2024; UNODC, Good Practices and Challenges with Respect to Beneficial Ownership Transparency.
[16] Attorney-General's Department (AGD), Reforming Australia's AML/CTF Regime Impact Analysis; FATF Recommendation 25: Transparency and beneficial ownership of legal arrangements
[17] Wolfsberg Group 2024 Statement on Effective Monitoring, Part I; GCFFC, Position Paper on Beneficial Ownership Data, AML/CTF Bill Explanatory memorandum.
[18] Too little useful intelligence. AUSTRAC Corporate Plan 2025-29; ACIC 2025-26 Corporate Plan; HKMA, Use of Artificial Intelligence for Monitoring of Suspicious Activities

3.2.4 TBML blind spots: Limited integration of trade data, poor cross-border analytics[19], and underdeveloped typology-specific reporting fields[20].

3.2.5 Capital markets laundering (MLTM): Inconsistent risk assessments and KYC at wholesale brokers; surveillance not tuned to ML typologies.[21]

3.2.6 CEF and scams: Speed[22] of funds movement overwhelms case-by-case responses; insufficient 24/7 joint operational muscle memory.

3.2.7 PF/sanctions evasion: Maritime/shipping registry risk and virtual assets (VA) channels require tighter coordination; gold/stablecoin vectors are emerging.[23]

3.2.8 Cryptocurrency laundering: Cybercrime-as-a-service professionalises and scales malicious activity using specialised tools and infrastructure; crypto laundering fragments and mixes illicit funds via tumblers and decentralised exchanges to evade detection.[24]

3.2.9 Asset recovery throughput: Recovery efficiency is constrained by low seizure-to-confiscation conversion rates and delays in cross-border asset returns; driven by coordination and case management frictions.[25]

4. Key Recommendations and Implementation Detail

4.1 Finish the legislative job (coverage, clarity, consistency)

4.1.1 DNFBPs: Phased commencement with sector-specific rules, AUSTRAC guidance[26] and starter program kits, onboarding controls, and uplift funding (subsidy[27] and shared utilities[28] for small practices).

4.1.2 Trusts and legal arrangements: Implement the latest international guidance for R.25 with a multi-source approach (trustee-held, registries, obliged entities), verification triggers, enforcement for non-compliance, and secure cross-border access mechanisms.[29]

---

[19] APGML Typology Report on Trade Based Money Laundering; Asian Development Bank (ADB), Transforming the Fight Against Trade-Based Money Laundering; World Customs Organization (WCO) Roundtable on Trade-based Money Laundering

[20] For example, SMRs do not have dedicated fields for trade invoice numbers, commodity codes, incoterms, shipping routes, customs declarations, or vessel identifiers. All of which are crucial for detecting TBML patterns.

[21] KPMG Global Banking Scam Survey 2025; OECD, The Limits of DeFi for Financial Inclusion; FCA, Assessing and reducing the risk of Money Laundering Through the Markets (MLTM).

[22] FATF Illicit Financial Flows from Cyber-enabled Fraud, GCFFC, Global Ledger's H1 2025 Report on Money Laundering Timing

[23] FATF, Complex Proliferation Financing and Sanctions Evasion Schemes; Joint APG-UNODC, Shipping Registries and PF Risk Factsheet; Atlantic Council - Gold's geopolitical comeback: How physical and digital gold can be used to evade US sanctions.

[24] Australian Signals Directorate (ASD), Annual Cyber Threat Report 2024-2025

[25] Egmont Group, Increasing FIU Effectiveness in the Asset Recovery Process: Phase II; Australian Institute of Criminology (AIC), A review of confiscation schemes in Australia; Home Affairs, Review of the Intergovernmental Agreement on the National Cooperative Scheme on Unexplained Wealth; Europol, Out of their hands: Europol and asset recovery.

[26] AUSTRAC issued its core guidance on 16 October 2025, with sector-specific guidance and starter program kits expected from late January 2026.

[27] Subsidised credits or grants for DNFBPs, especially small practices, to access AML/CTF tools and services (e.g., software, due diligence, monitoring, or training). This lowers upfront costs and accelerate uptake of compliant practices.

[28] Centralised, industry-wide platforms or services provided at low cost to small DNFBPs. Examples include: (1) shared transaction monitoring or screening services and (2) centralised verification databases.

[29] FATF, Guidance on Beneficial Ownership and Transparency of Legal Arrangements; GCFFC (Global Coalition to Fight Financial Crime), Beneficial Ownership Data position paper; OECD, Ending the Shell Game, Cracking down on the Professionals who enable Tax and White Collar Crimes.

4.1.3 Transfers of value and travel rule: Maintain technology-neutral drafting; issue operational guidance for virtual assets and instant payments; require attestation pathways where metadata[30] carriage is constrained.[31]

4.1.4 Proportionality and de-risking: Embed guidance to avoid indiscriminate de-risking of NPOs[32]/remitters; promote risk-mitigation (tiered controls, safe corridors) to preserve financial inclusion.[33]

4.2 Industrialise intelligence - data, analytics, AI (with safeguards)

4.2.1 National data platform: Establish a secure, federated “intelligence fabric” that supports entity resolution (people, companies, trusts, vessels, wallets), network analytics, pattern libraries (typologies), and case orchestration, integrated with agency systems.[34]

4.2.2 Explainable ML[35]: Adopt Wolfsberg-aligned “effectiveness” monitoring standards; pilot and scale explainable ML models with model-risk governance, challenge rounds, and regulator sandboxes; prioritise high-yield typologies (TBML, mule herding, nested VASPs, scams).[36]

4.2.3 Quality over quantity: Shift supervisory metrics from “alerts generated” to “outcomes delivered” (e.g., SMR-to-actionable-intelligence rate, timeliness, cross-case linkages).

4.2.4 Skills and safety: Fund joint analytic squads (AUSTRAC/AIC/ACIC/AFP/states/ASIC/ATO) and uplift workforce skills in data engineering, graph analytics, and AI assurance.

4.3 Out-cooperate adversaries (domestic and cross-border sharing)

4.3.1 COSMIC-style platform: Launch a MAS[37]-inspired, privacy-by-design platform enabling risk-based peer-to-peer sharing among prescribed institutions, with clear internal policies, request/response flows, publication thresholds, error-correction, and redress.[38]

4.3.2 Privacy enhancing technologies (PETs): Use secure multi-party computation and differential privacy to enable risk-signal exchange without revealing full customer data; standardise lexicon and risk codes.[39]

---

[30] In situations where technical or legal limitations prevent the complete or automatic transmission of transaction metadata (data about data), consider feasibility of permitting or mandating reporting entities to use attestation.
[31] AML/CTF Bill Explanatory Memorandum
[32] NPOs refer to non-profit organisations
[33] World Bank, De-risking in the Financial Sector; World Bank, Decline in Access to Correspondent Banking Services in Emerging Markets; AUSTRAC, National Risk Assessment: Terrorism Financing in Australia 2024
[34] ACIC Corporate Plan 2025-26; Future of Financial Intelligence Sharing (FFIS) Policy Paper; MAS Launches COSMIC Platform to Strengthen the Financial System’s Defence Against Money Laundering and Terrorism Financing.
[35] ML refers to machine learning in this context.
[36] Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity, Part I: Moving Beyond Automated Transaction Monitoring; Wolfsberg Statement on Effective Monitoring for Suspicious Activity, Part II: Transitioning to Innovation
[37] Monetary Authority of Singapore.
[38] MAS Launches COSMIC Platform to Strengthen the Financial System’s Defence Against Money Laundering and Terrorism Financing. Publication thresholds: COSMIC applies risk-based thresholds, publishing only information relevant to AML/CFT objectives and proportionate to risk, rather than all data, while protecting privacy. Error correction: Participants can flag or request amendments, enabling accurate, up-to-date data under MAS oversight. Redress: MAS-governed procedures provide a formal channel for disputes or concerns, ensuring data integrity and protection of legitimate interests.
[39] Future of Financial Intelligence Sharing (FFIS) Policy Paper; ABS, Industry Perspectives on Best Practices - Leveraging on Data Analytics and Machine Learning Methods for AML/CFT.

4.3.3 Cross-border frameworks: Expand bilateral/multilateral FIU channels; formalise joint targeting with customs authorities (WCO), APGML[40] partners, and Five Eyes; expedite reciprocal asset freezing and victim restitution on scams and ransomware.[41]

4.4 Make asset recovery routine (structure, powers, and practice)

4.4.1 National asset recovery coordination: Create a single tasking forum across AFP, AIC, ACIC, CDPP, AUSTRAC, ABF, ATO, state crime commissions, and public trustees to select priority targets, align tools (conviction/civil), and assign asset managers early.

4.4.2 Tooling and powers: Enable FIU "hold/freeze" powers time-boxed to judicial oversight; scale specialised financial investigators and forensic accountants; adopt best-practice management and disposal SOPs to preserve value.[42]

4.4.3 International networks: Systematically leverage CARIN-style networks and Egmont cooperation to trace assets; designate case liaisons in priority jurisdictions; align confiscation data standards to speed cross-border execution.

4.4.4 KPI discipline: Track asset restraint value, conversion rates to confiscation, time to disposal, and funds returned to victims or reinvested in capability.

4.5 Target the biggest gaps (focused programs)

4.5.1 TBML Fusion Cell

- Data and reporting: Introduce trade data elements in SMRs (commodity codes, incoterms[43], shipping identifiers, valuation anomalies); build anomaly detection on customs, trade finance, and open-source trade routes.
- Joint operations: Create rolling joint operations with ABF, ATO, AUSTRAC, banks/trade finance units, freight forwarders, and insurers; prioritise high-risk routes, dual-use goods, and third-country triangulation.[44]
- Guidance and red flags: Publish sector guidance for banks and logistics with dynamic red flags and case exemplars; extend to PF/sanctions evasion risks.

4.5.2 Scams and CEF Joint Ops

- 24/7 response: Institutionalise continuous "stop the loss" cells linking banks, platforms[45], telcos, payment gateways, and VASPs; standardise mule account freezes and recall protocols; pre-approve lawful notices for rapid data disclosure.
- Infrastructure takedown: Coordinate with platform trust & safety teams to disrupt scam infrastructure (domains, bots, deepfake content) and run synchronised public warnings.

[40] The Asia/Pacific Group on Money Laundering (APGML) is a FATF style regional inter-governmental body.
[41] FIU refers to Financial Intelligence Unit. WCO refers to World Customs Organization. Five Eyes refers to the intelligence-sharing alliance between Australia, Canada, New Zealand, the United Kingdom, and the United States.
[42] Egmont, Increasing FIU Effectiveness in the Asset Recovery Process: Phase II; United Nations Convention against Transnational Organized Crime; APEC, Best Practices in Investigating and Prosecuting Corruption; MAS, National Asset Recovery Strategy.
[43] Incoterms are international trade rules defining who (buyer or seller) is responsible for shipping, insurance, and customs costs. They are useful in SMRs to detect unusual trade patterns or money laundering risks.
[44] ADB, Transforming the Fight Against Trade-Based Money Laundering; WCO conducts Roundtable on Trade-based Money Laundering.
[45] Including non-obvious platforms such as running/fitness apps, beta test platforms, marketplaces, lifestyle/community apps, fake health apps, DeFi/gamified finance.

- Victim support: Fund “aftercare” and rapid referrals; reduce repeat[46] victimisation with behavioural cues, bank prompts, and educational nudges at point-of-risk.

4.5.3 Virtual assets and instant payments

- Supervision: Risk-based thematic reviews on cross-chain bridges, mixers, privacy coins, stablecoins, and OTC brokers; test travel-rule compliance at scale with interop pilots.[47]
- Forensics at speed: Expand blockchain analytics reach (cross-chain heuristics, wallet clustering, typology libraries); enable expedited freezing via judicial on-call rosters.[48]

4.5.4 Capital markets (Money Laundering Through Markets)

- Controls: Uplift KYC/CDD in wholesale brokers; tune surveillance to ML typologies (layering via illiquid instruments, wash trades[49] to obfuscate provenance[50], cross-venue cycling[51]).
- SMR quality: Improve SMR specificity (instrument, venue, beneficial owner linkages) and feedback loops from investigators to compliance teams.

4.5.5 Proliferation financing and sanctions evasion

- Maritime risk: Screen shipping registries/vessel histories (flag hopping, AIS[52] gaps, manager/operator links); mandate enhanced due diligence for maritime exposures, insurers, brokers, and trade financiers.[53]
- Non-traditional stores of value: Address gold and gold-backed stablecoin channels through targeted guidance and reporting triggers.

4.5.6 Real estate and professional enablers

- Gatekeeper programs: For lawyers, conveyancers, accountants, trust and company service providers, issue templated programs, sector-specific red flags (client layering, “loan back” schemes, undervaluation/overvaluation), and targeted sector assurance.
- Digital settlement risk: With PEXA and lenders, enhance anomaly detection (rapid flips, offshore PEP[54] links, nominee owners, cash-intensive buyers).[55]

4.6 Beneficial ownership - make it usable

4.6.1 Structured data: Implement interoperable, open standards for beneficial ownership records with unique identifiers, role taxonomy for trust parties

[46] Singapore Police Force, Restricting Access To Facilities For Scam Mules
[47] Elliptic, The state of cross-chain crime 2025; FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers; Cambridge Centre for Alternative Finance (CCAF), 2nd Global Cryptoasset Regulatory Landscape Study.
[48] GCFFC, Global Ledger’s H1 2025 Report on Money Laundering Timing; Chainalysis, 2025 Crypto Crime Report.
[49] Trades where the same party (or colluding parties) buys and sells the same financial instrument. This is often at the same price, creating the illusion of market activity or moving funds without real economic exposure.
[50] To disguise the origin of the assets.
[51] Executing trades across multiple trading venues (e.g. different exchanges, dark pools, or OTC platforms) to further complicate detection and audit trails.
[52] AIS (Automatic Identification System) is a global tracking system showing a ship’s identity, location, and route. In AML and sanctions contexts, “AIS gaps” occur when a vessel disables or manipulates its signal to hide movements. This is often to mask ship-to-ship transfers, high-risk routing, or false flagging.
[53] APGML, Joint APG-UNODC Shipping Registries and PF Risk Factsheet.
[54] PEP refers to politically exposed persons.
[55] AUSTRAC Money Laundering NRA 2024; GFI, Money Laundering Risks in Commercial Real Estate; AUSTRAC, Major banks in Australia risk assessment.

(settlor, trustee, protector, beneficiary, controller), and machine-readable change logs.

4.6.2 Verification: Hybrid verification (documentary, digital, cross-dataset reconciliation) with risk-tiered checks; escalate professional trustee supervision.[56]

4.6.3 Access: Provide legitimate-interest access with logging, proportional redaction, and audit; enable cross-border requests through standardised APIs with judicial/administrative gateways.[57]

4.6.4 Feedback loop: Allow competent authorities to flag inaccuracies; embed sanctions and remediation SLAs[58] for corrections.

4.7 Technology and AI (safe, explainable, and effective)

4.7.1 Governance: Adopt a model-risk framework for AML AI; documented purpose, training data lineage, bias testing, stability monitoring, human-in-the-loop, and audit trails admissible in court.

4.7.2 Architecture: Use a layered approach; data lakehouse[59], MDM[60]/entity resolution, graph analytics, and ML services; secured by zero trust and confidential computing where appropriate.

4.7.3 Procurement: Favour modular, standards-based tooling to avoid vendor lock-in; co-develop analytic SOPs with agencies and FIs; support regulator sandboxes for new typologies.

5. Measuring Effectiveness – KPIs that matter

5.1 Outcomes over inputs. Establish a national dashboard reported every six months to Parliament:

5.1.1 Asset denial: value restrained; restraint-to-confiscation conversion rate; time to confiscation; value returned to victims or reinvested.

5.1.2 Intelligence yield: SMR-to-investigative-lead rate; lead-to-outcome rate (arrest/charge/disruption); median time from SMR to action.

5.1.3 Scam harm: gross losses; recovered funds; time-to-freeze; reduction in repeat victimisation.

5.1.4 TBML/PF disruptions: number of disrupted trade corridors; high-risk shipment interdictions; sanctions-evasion typology closures[61].

5.1.5 Supervision effectiveness: proportion of high-risk sectors under active supervision; remediation cycle times; enforcement outcomes tied to risk.

5.1.6 International cooperation: cross-border requests processed; joint cases with partner FIUs; time to reciprocal orders.

---

[56] FATF, Guidance on Beneficial Ownership and Transparency of Legal Arrangements.
[57] Treasury, Regulatory reform to reduce red tape and ease burden on businesses.
[58] SLAs refer Service Level Agreements.
[59] A data lakehouse is a modern data architecture combining a data lake's ability to store large, raw datasets with a data warehouse's structured, searchable, and governed analytics. It enables centralised storage, advanced analytics and ML, and integration with graph analytics, and ML services for entity resolution and risk detection.
[60] MDM (Master Data Management) creates a single, accurate view of key entities, such as customers, accounts, or counterparties, across systems. In AML/CTF, it helps merge duplicate records, link related entities, and enable reliable analytics for risk detection.
[61] DFAT, Advisory Note – Sanctions & proliferation financing.

5.1.7 FATF effectiveness: improved ratings on Immediate Outcomes; closure of key recommended actions (KRA) items.

6. Governance, Accountability, and Resourcing

6.1 Whole-of-government board: A standing Economic Crime Board chaired at Deputy Secretary level to prioritise targets, approve joint operations, and remove roadblocks; include industry representatives for public-private sector partnerships (PPP) decisions.

6.2 Funding model: Multi-year capability uplift (analytics, specialist investigators, legal officers, digital forensics) with partial allocation[62] of confiscated proceeds to sustain the asset recovery pipeline.[63]

6.3 Public transparency: Publish an annual "State of Financial Crime" report or "Financial Crime Harm Index[64]", integrating law enforcement outcomes, supervisory insights, private-sector metrics, and community harm measures.

6.4 Proposed roadmap and milestones (approx. 36 months)

Phase	**One**	**Two**	**Three**
Legislative & policy	Issue sector guidance (DNFBPs, virtual assets, transfers)	Trusts verification; beneficial ownership (BO) usability standards	National rollout; legislative refinements from early lessons
Intelligence & tech	Stand up joint design team; approve AI/ML[65] governance; launch data model and entity resolution pilots	Scale explainable ML for top typologies; integrate cross border data feeds; PETs pilots in PPP[66]	Full national analytics fabric; model libraries; continuous red team/blue team tuning
PPP & sharing	Design COSMIC-style platform parameters; draft internal policies	Launch voluntary phase with major banks, PSPs[67], VASPs; publish red flags packs	Expand to DNFBPs; cross border connectors; standardised feedback loops
TBML & PF	Define enhanced SMR fields; create TBML Fusion Cell; select priority corridors	Deploy anomaly analytics; joint ops with customs/trade	Mature cross border TBML exchanges; measurable corridor derisking[68]

[62] Using part of the money recovered from criminals to fund ongoing asset recovery efforts.
[63] MAS, National Asset Recovery Strategy; AIC, A review of confiscation schemes in Australia; Egmont Group, Increasing FIU Effectiveness in the Asset Recovery Process: Phase II; NSW, Criminal Asset Confiscation Team - new taskforce to target the ill-gotten wealth of organised crime 'kingpins'; World Bank, Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes.
[64] Similar to the Cambridge Crime Harm Index (CCHI), the Committee may consider developing the first system that measures the seriousness of financial crime harm to victims, and not just the number of officially recorded crimes.
[65] Artificial intelligence and machine learning (AI/ML). Not to be confused with money laundering and terrorism financing (ML/TF).
[66] ABS, Industry Perspectives on Best Practices - Leveraging on Data Analytics and Machine Learning Methods for AML/CFT; GCFFC, A Risk Scoring Model for Managing Money Laundering Transactions; CNA, INTERPOL partners Singapore agencies for breakthroughs in enforcement tools.
[67] Refers to Payment Service Providers.
[68] ADB, Transforming the Fight Against Trade-Based Money Laundering; APGML Typology Report on Trade Based Money Laundering; WCO conducts Roundtable on Trade-based Money Laundering.

		finance; maritime risk program	
Scams/CEF	Establish 24/7 joint response; standardise stop the loss SOPs	Infrastructure takedown cadence with platforms; victim aftercare scaling	Material reduction in losses and time to freeze; repeat victimisation down
Asset recovery	National coordination forum; common KPIs; early asset manager assignment	Freeze powers optimised; cross border case templates; disposal SOPs	Confiscation conversion rate >50%; time to confiscation down >30%[69]

7. Risk Management and Safeguards

7.1 Privacy and proportionality: Legitimate interest access and PETs guardrails; DPIAs for new data uses; role-based access and immutable audit logs.[70]

7.2 Model risk: Independent validation; challenger models; bias and drift testing; clear override/escalation protocols.

7.3 Derisking avoidance: Supervisory guidance that mandates calibrated, documented risk-mitigation for NPOs and remitters; escalation to safe-corridor models before termination.[71]

7.4 Legal robustness: Legal sign-off on AI-assisted evidence trails, chain of custody for digital artifacts, and admissibility preparation.

8. Illustrative Case Examples (indicative)[72]

8.1 BEC rings: Joint 24/7 cell freezes mule networks within hours; cross-institution sharing surfaces a master controller; funds recovered before layering.

8.2 Crypto hack timing: On-chain analytics flag abnormal bridge flows in minutes; urgent orders freeze assets mid-route; seized funds returned to victims via civil recovery.

8.3 TBML: Over/under-invoicing detected by combined customs/finance data; vessel manager linked to PF network; shipments seized, counterparties debanked.

8.4 Real estate layering: Structured beneficial ownership (BO) data and DNFBP red flags reveal nominee owners and round-tripped loans; civil confiscation proceeds fund further investigations.

9. What Success Looks Like by 2028

9.1 Raised FATF effectiveness ratings; closed long-standing gaps in DNFBPs and beneficial ownership transparency for legal arrangements.

[69] Illustrative example (indicative)
[70] Data Protection Impact Assessments refer to formal reviews that identify and minimise privacy risks when introducing new data uses, ensuring legal compliance and responsible, auditable handling of personal or sensitive data.
[71] This safeguard targets derisking, where banks cut off high-risk clients (e.g., NPOs or remitters) instead of managing risk. It mandates documented, proportionate controls and, where needed, safe-corridor arrangements, as account closure can prevent law enforcement from tracing funds.
[72] Illustrative case examples (indicative) are hypothetical scenarios showing how proposed reforms could be applied to real-world financial crime situations. They demonstrate the potential operational impact of our proposed plan to strengthen Australia's law enforcement capability against financial crime.

9.2 Measurable harm reduction: fewer scam losses and faster recovery; shorter time from alert to disruption; higher confiscation conversion rates.

9.3 A trusted, privacy-safe PPP fabric that scales intelligence sharing domestically and across borders, with PETs operationalised.

9.4 A workforce and toolset calibrated to AI-accelerated, cross-border criminality: faster, more precise, and demonstrably fair.

10. Conclusion

Australia can convert reform intent into operational outcomes by finishing legislative coverage, scaling a privacy-by-design information-sharing fabric, industrialising intelligence with data analytics and explainable AI, making asset recovery routine, and measuring what matters.

The proposed roadmap outlined above focuses on the highest-yield gaps with clear milestones and safeguards. Delivering it will materially reduce criminal profits, protect victims, lift international standing, and strengthen national resilience.

Summary of key points

- Complete tranche two and trusts transparency with practical guidance and pacing.
- Launch a COSMIC-style PPP platform with PETs and strong governance.
- Shift monitoring to effectiveness with explainable ML, entity resolution, and graph analytics.
- Make beneficial ownership data structured, verified, and usable across borders.
- Institutionalise asset recovery coordination and reinvest proceeds into capability.
- Stand up a TBML Fusion Cell; tighten PF/sanctions evasion controls.
- Build 24/7 scams/CEF joint response; reduce losses and time-to-freeze.
- Introduce capital-markets MLTM program with wholesale uplifts.
- Publish outcome KPIs; report transparently every six months.
- Govern with privacy, fairness, and legal robustness at the core.

About the Author

Crispin Yuen, CAMS-Audit, CISSP, CISA

Director

Custos Advisory

Crispin Yuen is an award-winning financial crime risk and compliance specialist with over 20 years' experience spanning governance, anti-money laundering and counter terrorism financing (AML/CTF), sanctions, fraud, cybercrime, investigations, and regulatory remediation. He combines technical depth with pragmatic delivery to meet complex, group-wide agendas and to help organisations navigate evolving regulatory expectations.

Crispin's background bridges financial institutions and professional services. He has in-depth remediation experience addressing sanctions control and AML/CTF deficiencies arising from OFAC and AUSTRAC enforcement actions - experience rare in the Asia-Pacific region. His approach emphasises strengthened risk assessment, proportionate controls, transparent documentation, and verifiable assurance, ensuring reforms are both regulator-ready and operationally sustainable.

He has led trade-surveillance and forensic investigations into insider trading, market manipulation, and market-integrity breaches, using data analytics and communications analysis to build regulatory referrals and evidentiary submissions. He designed and implemented competition and consumer law compliance programs to prevent cartel behaviour and price-fixing, and has supported cartel investigations. In addition to financial markets work, he has managed fraud and embezzlement investigations and strengthened anti-fraud controls. He has partnered with law enforcement agencies on cybercrime and account-takeover cases involving share-registry accounts, tracing transactions and supporting asset recovery. He has also conducted sensitive workplace investigations, including sexual harassment, and implemented whistleblower reporting, protection, and escalation frameworks to uphold robust governance.

Crispin has developed strong, collaborative relationships with regulators and law enforcement agencies. He has shared his insights as an industry witness before the Australian Parliamentary Joint Committee on Law Enforcement's inquiry into financial-related crime (2015). In 2022, he was invited to a United Nations expert roundtable in Vienna, convened by the UN Ad Hoc Committee on Cybercrime under UN General Assembly resolution 75/282. His contributions helped inform the development and eventual adoption of the United Nations Convention against Cybercrime by the UN General Assembly in 2024.

Recognised as an expert by the Global Initiative Against Transnational Organized Crime, he joined its Global Organized Crime Steering Committee in 2022, working with representatives from the United Nations and delegations to the Conference of the Parties to the UN Convention against Transnational Organized Crime. In 2024 he co-authored *"Intersections: Building Blocks of a Global Strategy Against Organized Crime"* and continues to advise on financial-crime threats linked to organised crime, identifying good practices and policy recommendations. In 2024 he was also invited to join the Vancouver Anti-Corruption Institute (VACI) as a VACI Expert.

Crispin has spoken at events convened by the China Banking Association; Regulating the Game (Australia); Bank Negara Malaysia and the Malaysian Association of Money Services Businesses; New Zealand Police; the Institute of International Banking Law & Practice; and VACI, part of the International Centre for Criminal Law Reform, a UN Crime Prevention and Criminal Justice Programme Network of Institutes. Crispin has written for LexisNexis and Thomson Reuters, and he has been interviewed on financial crime matters by ABC News, South China Morning Post, and BBC News.

Crispin has served on the ACAMS Australasian Chapter Board for over 18 years and is part of ACAMS' global teaching faculty. His qualifications include Certified Anti-Money Laundering Specialist (CAMS), Certified Advanced AML Audit Specialist (CAMS-Audit), Certified Information Systems Security Professional (CISSP), and Certified Information Systems Auditor (CISA). He co-authored study guides and exam questions for CAMS, CAMS-Audit, and the Certified Global Sanctions Specialist (CGSS). He authored the book *"FATF Review of Standards – 2010-2011"* (available on Amazon) and has taught Risk Management and Compliance Monitoring at Nanyang Polytechnic, and International Financial Crime at the University of Sydney.